Neue Brennpunkte im Verhältnis von Informationstechnologien, Datensammlungen und flexibilisierter Rechtsordnung

Weber, Rolf H ; Wolf, Christoph A ; Heinrich, Ulrike I

www.jusletter.ch

Prof. Dr. Rolf H. Weber / Christoph A. Wolf / Ulrike I. Heinrich

Neue Brennpunkte im Verhältnis von Informationstechnologien, Datensammlungen und flexibilisierter Rechtsordnung

Vorratsdatenspeicherung – Staatstrojaner – Geolokalisierungsdaten

Die Informationstechnologie mit ihren rasanten Entwicklungen stellt das Recht immer wieder auf die Probe. Im Beitrag untersuchen die Verfasser drei spezifische Teilbereiche, welche in letzter Zeit besonderen Diskussionsbedarf hervorgerufen haben, nämlich die Vorratsdatenspeicherung im Zeichen der Verbrechensbekämpfung sowie der Gefahrenabwehr, der Einsatz sog. Staatstrojaner zu denselben Zwecken sowie die Herausforderungen angesichts der Entwicklungen im Bereiche der mobilen Ortungsdienste. Der Beitrag zeigt in kritischer Würdigung auf, wie die Rechtsordnung mit diesen Phänomenen umgeht.

Rechtsgebiet(e): Datenschutz; Informatik und Recht; Beiträge

Zitiervorschlag: Rolf H. Weber / Christoph A. Wolf / Ulrike I. Heinrich, Neue Brennpunkte im Verhältnis von Informationstechnologien, Datensammlungen und flexibilisierter Rechtsordnung, in: Jusletter 12. März 2012

ISSN 1424-7410, www.jusletter.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 Editions Weblaw

Inhaltsübersicht

A. Einleitung

[Rz 1] Neue technologische Entwicklungen stellen das Recht nicht selten vor schwierige Herausforderungen; die Rechtsordnung ist deshalb gezwungen, auf unsicherer Grundlage zu reagieren. Die Antizipation zukünftiger Entwicklungen ist oft kaum möglich und eine vorsorgliche Regelung an sich (noch) nicht regelungsbedürftiger Aspekte trifft auf den berechtigten Einwand der Vermeidung einer Überregulierung, weshalb sich Probleme zuerst in der Praxis manifestieren müssen, bevor der Gesetzgeber gegebenenfalls ordnend eingreift. Diese Einschätzung gilt in besonderem Masse auch für Entwicklungen in der Informationstechnologie.

[Rz 2] Die nachfolgenden Ausführungen orientieren sich an drei Beispielen: (1) Mittels der Vorratsdatenspeicherung kann es Behörden theoretisch möglich gemacht werden, fast unbegrenzt aus der Vergangenheit Daten über eine Person zu erheben. (2) Der Einsatz von Malware zur Überwachung von Personen eröffnet bisher ungeahnte Möglichkeiten der Spionage und weckt damit auch entsprechende Befürchtungen. (3) Das vermehrte Angebot an Geolokalisierungsdiensten ermöglicht es, Informationen über den momentanen Aufenthaltsort einer Person an soziale Netzwerke zu senden, um andere Personen über diesen Umstand zu informieren oder um in den Genuss besonderer Vergünstigungen zu gelangen.

[Rz 3] Die beschriebenen Entwicklungen haben gemeinsam, dass sich die staatlichen Regelungsmechanismen diesbezüglich entweder erst im Entwicklungsstadium befinden oder sich die Frage stellt, ob sie an neue Umstände anzupassen sind. Nachfolgend sollen die drei genannten Problembereiche beschrieben, in ihren rechtlichen Kontext gestellt sowie Ansätze zu Lösungsvorschlägen für die eintretenden Probleme und Herausforderungen entwickelt werden.

B. Vorratsdatenspeicherung

1. Begriff und Problematik

[Rz 4] Der Begriff der Vorratsdatenspeicherung bezeichnet die durch staatliche Vorschriften gebotene Protokollierung sämtlicher anfallender Telekommunikationsverbindungsdaten durch die Anbieter von Diensten wie Telefonie, SMS oder Internet, welche bei Vorliegen bestimmter Voraussetzungen Strafverfolgungsbehörden auf entsprechendes Begehren hin zur Verfügung gestellt werden.[1] Der Zweck der Vorratsdatenspeicherung liegt in der möglichen Verwendung der Daten namentlich zur Aufklärung von über das Internet oder andere Kommunikationsformen begangener Straftaten[2] sowie der möglichen Abwehr entsprechender Gefahren, etwa durch terroristische Aktivitäten.

[Rz 5] Betroffen von der Vorratsdatenspeicherung im hier verstandenen Sinn sind vorab sog. Randdaten, d.h. Daten über Zeitpunkt, Länge, Teilnehmer eines Telefongespräches oder Absender und Empfänger einer E-Mail, nicht aber deren Inhalt.[3] Vorratsdatenspeicherung bedeutet weiter, dass die fraglichen Daten von Privaten, in der Regel also von den jeweiligen Dienstleistungsanbietern, für die Strafverfolgungsbehörden zur Verfügung zu halten sind, d.h. in Frage steht eine dezentrale Speicherung, die Herausgabe an die Behörde findet nur auf Gesuch hin statt.

[Rz 6] Die Vorratsdatenspeicherung kann für die interessierten Behörden zweifellos erhebliche Verbesserungen in der Aufklärung und Verhütung von Delikten mit sich bringen, weil im Gegensatz zu den üblichen Überwachungsmethoden nicht erst die nach Vorliegen eines begründeten Verdachts,[4] sondern auch schon in einem früheren Stadium angefallenen Daten einverlangt werden können. Die Vorratsdatenspeicherung birgt indessen auch Gefahren bzw. weckt Ängste und Befürchtungen. So wird seitens der Internetnutzer sowie der Politik kritisiert, es werde die gesamte Bevölkerung unter Generalverdacht gestellt;[5] zudem werden die finanziellen

---

[1] Vgl. auch Mark Seibert, Freiheit oder Sicherheit?; Die Umsetzung der Vorratsdatenspeicherung in Deutschland, 2009, S. 3.

[2] Anschaulich dazu der dem Urteil des Bundesgerichts 6B_766/2009 vom 8. Januar 2010 zugrunde liegende Sachverhalt.

[3] Vgl. die Definition nach Art. 5 der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (hernach: Richtlinie).

[4] Vgl. dazu etwa den Wortlaut von Art. 269 Abs. 1 lit. a StPO.

[5] Vgl. etwa ‹http://www.fr-online.de/politik/vorratsdatenspeicherung-von-millionen-fdp-warnt-vor-generalverdacht-,1472596,4866848.html›,

Folgen der Speicherung entsprechender Datenmengen beanstandet.[6]

2. Rechtslage in der EU

2.1. Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten

[Rz 7] Im Lichte der zunehmenden Bedrohungslage seitens von Terroristen, welche über moderne Kommunikationskanäle miteinander in Verbindung treten, aber auch angesichts der Möglichkeit, herkömmliche Straftaten vermehrt im Internet zu begehen, begann sich in der EU das Bewusstsein durchzusetzen, die vorsorgliche und anlasslose Speicherung von bestimmen Daten könnte die Ermittlungstätigkeit sowie die Gefahrenabwehr vereinfachen oder zum Teil gar erst ermöglichen. Insbesondere nach den Terroranschlägen vom 7. Juli 2005 in London bekam die seit 2001 bestehende Forderung nach einer einheitlichen Regelung der Vorratsdatenspeicherung Aufwind.[7] Am 17. September 2005 stimmte schliesslich das EU-Parlament und am 21. Februar 2006 der Ministerrat der Richtlinie zu.

[Rz 8] Die Richtlinie, welche keine direkten Wirkungen auf die EU-Bürger entfaltet, sondern lediglich die Mitgliedsstaaten zu einer bestimmten Gesetzgebung veranlasst,[8] sieht in Art. 6 vor, dass bestimmte Kategorien von Daten, wie in Art. 5 der Richtlinie festgelegt, mindestens sechs Monate und maximal zwei Jahre auf Vorrat zu speichern sind. Die Regelung der Voraussetzungen des Zuganges staatlicher Stellen zu den gespeicherten Daten wird den Mitgliedstaaten überlassen.[9] Den Mitgliedstaaten wurde Frist bis maximal 15. März 2009 eingeräumt, um die entsprechenden Vorschriften zu erlassen.[10]

2.2. Implementierung in nationales Recht

[Rz 9] Obwohl die Richtlinie die Umsetzung der Vorgaben in nationales Recht bis spätestens 15. März 2009 vorsah, gab es einige Mitgliedstaaten, welche die Umsetzung versäumten oder bis heute nicht vorgenommen haben. In Deutschland wurde auf den 1. Januar 2008 ein Umsetzungsgesetz in Kraft gesetzt,[11] welches das Bundesverfassungsgericht am 2. März 2010 indessen als in wesentlichen Teilen verfassungswidrig und daher nichtig beurteilt hat.[12] Ein ähnliches Bild zeigt sich auch etwa in Tschechien[13] sowie in Rumänien.[14] Während z.B. in Frankreich fristgemäss schon im Januar 2006 ein entsprechendes Umsetzungsgesetz entstand, welches eine Aufbewahrungszeit von zwölf Monaten vorsieht,[15] hat Schweden sich bisher geweigert, ein solches Gesetz zu erlassen, weshalb der Europäische Gerichtshof mit Urteil vom 4. Februar 2010 Schweden wegen Vertragsverletzung verurteilt hat.[16] Somit zeigt sich innerhalb der EU kein einheitliches Bild, weil in einigen Staaten überhaupt keine entsprechende Regelung besteht, während andere Staaten eine verhältnismässig weitgehende Speicherdauer vorsehen.

2.3. Gerichtsentscheide

[Rz 10] Wie bereits erwähnt, hat die Richtlinie, aber auch ihre Umsetzung in nationales Recht, verschiedentlich die Gerichte beschäftigt. Auf europäischer Ebene verwarf der Europäische Gerichtshof mit Urteil vom 10. Februar 2009 eine Nichtigkeitsklage Irlands gegen die Richtlinie, welche sich auf das Fehlen einer geeigneten Rechtsgrundlage stützte.[17]

[Rz 11] In Deutschland formierte sich schon früh breiter Protest gegen die voraussetzungslose Speicherung von Daten.[18] Fünf Tage nach der Unterzeichnung der Umsetzungsnormen zur Richtlinie wurde beim Bundesverfassungsgericht eine Verfassungsbeschwerde gegen die betroffenen Rechtsnormen eingereicht, die später die Unterstützung von über 30'000 Bürgern fand. Nachdem schon einstweilige Anordnungen die Vorratsdatenspeicherung zwar nicht ausgeschlossen, aber erhöhten Voraussetzungen unterstellt hatten,[19] hat das

besucht am 3. Februar 2012.

6 Birgit Kolb, Vorratsdatenspeicherung, unter Berücksichtigung der TKG-Novelle 2011, Salzburg 2011, S. 149.

7 Dorothee Szuba, Vorratsdatenspeicherung; Der europäische und deutsche Gesetzgeber im Spannungsfeld zwischen Sicherheit und Freiheit, Frankfurt a.M., 2011, S. 50.

8 Art. 288 des Vertrages über die Arbeitsweise der Europäischen Union (ehemals Art. 249 des Vertrages zur Gründung der Europäischen Gemeinschaft).

9 Richtlinie (FN 3), Art. 4.

10 Am 13. April 2006 wurde die Richtlinie sodann im Amtsblatt der Europäischen Union publiziert.‹http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2006:105:SOM:DE:HTML›, besucht am 27. Januar 2012.

11 Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmassnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, abrufbar unter , besucht am 27. Januar 2012

12 Vgl. dazu sogleich Rz. 11.

13 *Data Retention in Telecommunications Services*, 2011/03/22 - Pl. ÚS 24/10.

14 *Entscheidung 1258* vom 8. Oktober 2009.

15 Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, abrufbar unter ‹http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006053177›, besucht am 27. Januar 2012.

16 Urteil des Europäischen Gerichtshofes vom 4. Februar 2012 in der Rechtssache C-185/09, abrufbar unter ‹http://curia.europa.eu/juris/document/document.jsf?docid=79860&mode=lst&pageIndex=1&dir=&occ=first&part=1&text=&doclang=DE&cid=729998›, besucht am 27. Januar 2012.

17 Urteil des Europäischen Gerichtshofes in der Rechtssache C-301/06 (Irland gegen Europäisches Parlament und Rat der Europäischen Union) vom 10 Februar 2009.

18 Vgl. etwa «Proteste gegen Vorratsdatenspeicherung», in: Frankfurter Allgemeine Zeitung vom 7. November 2009 (abrufbar unter ‹http://www.faz.net/aktuell/politik/inland/datenschutz-proteste-gegen-vorratsdatenspeicherung-1491762.html›, besucht am 27. Januar 2012).

19 Beschluss des Bundesverfassungsgerichts vom 11. März 2008 in der Rechtssache 1 BvR 256/08, abrufbar unter ‹http://www.

Bundesverfassungsgericht mit Urteil vom 2. März 2010 die fraglichen Umsetzungsnormen für nichtig erklärt.[20] Das Gericht beurteilte die vorgesehene sechsmonatige Speicherfrist zwar nicht als per se unvereinbar mit Art. 10 des deutschen Grundgesetzes, welcher die Unverletzlichkeit des Brief-, Post- und Fernmeldegeheimnisses statuiert, bemängelte aber das Fehlen von klaren Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes.

2.4. Ausblick

[Rz 12] In Deutschland sind weiterhin Diskussionen im Gange, wie eine gemässigte Vorratsdatenspeicherung dennoch eingeführt werden könnte, welche aber bis jetzt noch zu keinen konkreten Massnahmen geführt haben. Im Januar 2011 präsentierte die Justizministerin Leutheusser-Schnarrenberger einen Vorschlag, welcher unter anderem eine siebentägige Aufbewahrungsfrist für Randdaten des Internetverkehrs vorsieht.[21] Weil Deutschland den Verpflichtungen aus der Richtlinie nicht vollständig nachgekommen ist, hat die EU-Kommission ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet.[22]

3. Rechtslage in der Schweiz

3.1 Derzeitige Rechtslage

[Rz 13] In der Schweiz wird die anlasslose Speicherung von Randdaten auf bundesrechtlicher Ebene durch Art. 15 Abs. 3 BÜPF geregelt. Art. 12 Abs. 2 BÜPF sieht eine analoge Regelung für Daten des Postverkehrs vor. Die Speicherfrist beträgt einheitlich sechs Monate; die Speicherung ist von den Service-Anbietern selber vorzunehmen. In Art. 27 VÜPF werden die zu speichernden Daten im Einzelnen umschrieben. Die Edition entsprechender Daten durch die Strafverfolgungsbehörden ist in Art. 273 StPO geregelt. Demnach kann die Staatsanwaltschaft die entsprechenden Daten einfordern, sofern ein dringender Verdacht auf ein Verbrechen,[23] ein Vergehen[24] oder eine Übertretung nach Art. 179^{septies} StGB[25] besteht, die Schwere der Straftat die Überwachung rechtfertigt und die bisherigen Untersuchungshandlungen erfolglos geblieben sind oder die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden. Die entsprechende Anordnung durch die Strafuntersuchungsbehörde muss durch das Zwangsmassnahmegericht genehmigt werden.[26]

[Rz 14] Während in den europäischen Nachbarländern teils kontroverse und vereinzelt heftige Auseinandersetzungen die Einführung der Vorratsdatenspeicherung begleiteten,[27] scheint die Diskussion in der Schweiz bedeutend nüchterner geführt worden zu sein. Zwar verlief die Behandlung der Angelegenheit in der parlamentarischen Debatte nicht unumstritten, doch fand die Regelung schliesslich eine überwiegende Mehrheit in den Räten.[28] Weder kam es zu Demonstrationen, noch stand die Ergreifung eines Referendums zur Debatte.

[Rz 15] Wenngleich das geltende BÜPF keine eigentlichen Sanktionen bei Vernachlässigung oder gar bewusstem Unterlassen der Aufbewahrungspflicht vorsieht, hat das Bundesgericht klargestellt, dass Widerhandlungen nicht ohne Folgen sein können, indem es im Januar 2010 entschieden hat, dass die Löschung der durch den Server automatisch gespeicherten IP-Adressen – im vorliegenden Fall handelte es sich um den Betreiber eines Internet-Diskussionsforums, welchen eine Aufbewahrungspflicht traf – eine Begünstigung im Sinne von Art. 305 StGB darzustellen vermag.[29]

3.2 Handlungsbedarf in der Schweiz?

[Rz 16] Wie bereits dargelegt, befindet sich die Schweiz mit ihrer derzeitigen Regelung der Vorratsdatenspeicherung hinsichtlich der Aufbewahrungsdauer im europäischen Mittelfeld. Die Gerichte beschäftigt hat die Vorratsdatenspeicherung – soweit ersichtlich – eher selten. Im Hinblick auf die zunehmende Sensibilisierung der Politik auf internetbasierte Kriminalität – namentlich auch die in den letzten Jahren erneut aufgetretenen Fälle von Kinderpornographie – formierte sich allerdings der Ruf nach einer Verstärkung der Überwachungsmassnahmen. Im Ständerat wurde schon 2005 ein Postulat eingereicht, welches eine Verlängerung der Aufbewahrungsdauer in unbestimmter Höhe forderte,[30] 2006 folgte sodann eine Motion, welche unter anderem eine Verdoppelung der Aufbewahrungsfrist von Art. 15 Abs. 3 BÜPF auf zwölf Monate sowie eine Strafbestimmung für den Fall der Missachtung dieser Vorschrift verlangte.[31]

---

bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr025608.html›, besucht am 27. Januar 2012.

[20] Urteil des Bundesverfassungsgericht vom 2. März 2010 in den Rechtssachen 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, abrufbar unter ‹https://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html›, besucht am 27. Januar 2012.

[21] Vgl. ‹http://www.bmj.de/SharedDocs/Kurzmeldungen/DE/2011/20110117_Leutheusser_Schnarrenberger_legt_Eckpunkte_zu_Quickfreeze_vor.html›, besucht am 27. Januar 2012.

[22] «EU leitet Verfahren gegen Deutschland ein», in Die Welt vom 22. Juni 2011 (abrufbar unter ‹http://www.welt.de/politik/deutschland/article13443492/EU-leitet-Verfahren-gegen-Deutschland-ein.html›, besucht am 27. Juni 2012).

[23] Art. 10 Abs. 2 StGB.

[24] Art. 10 Abs. 3 StGB.

[25] Missbrauch einer Fernmeldeanlage.

[26] Art. 273 Abs. 2 StPO.

[27] Vgl. dazu die Ausführungen oben Rz. 11 und 12.

[28] AB NR 2000 1208; AB SR 2000 721.

[29] Urteil des Bundesgerichts 6B_766/2009 vom 8. Januar 2010, E 3.4 f.

[30] Postulat 05.3006 der Sicherheitspolitischen Kommission des Ständerates, eingereicht am 21. Februar 2005.

[31] Motion 06.3170 von Rolf Schweiger, eingereicht am 24. März 2006.

[Rz 17] Diese Forderungen haben in den Vorentwurf des revBÜPF insoweit Eingang gefunden, als einerseits die Aufbewahrungsfrist auf zwölf Monate verlängert[32] und andererseits eine entsprechende Strafbestimmung aufgenommen werden soll.[33] Der Bericht zum Vorentwurf begründet denn die Verlängerung auch vorab mit der *auf Erfahrung beruhenden Feststellung*, dass sechs Monate für erfolgreiche Nachforschungen zu kurz bemessen seien.[34] In der Vernehmlassung gingen die Reaktionen auf die vorgeschlagene Änderung der Speicherdauer auseinander; während einige Teilnehmer die Verlängerung ausdrücklich begrüssten, lehnten andere dieses Anliegen ab oder vermissten zumindest eine schlüssige Begründung dafür.[35]

[Rz 18] Aufgrund der Ergebnisse der Vernehmlassung ist noch nicht absehbar, ob der künftige Entwurf des Bundesrates die Verlängerung der Speicherfrist übernehmen wird. Fest steht indessen, dass eine solche Verlängerung für die Schweiz eine gemessen an den Nachbarstaaten weitreichende Speicherdauer bedeuten würde. Eine Ausdehnung der Speicherdauer lässt sich indessen u.E. nicht ohne weiteres mit verfassungsrechtlich garantierten Grundrechten (vor allem dem Schutz der Privatsphäre im Sinne von Art. 13 BV) vereinbaren. Wenngleich die Anliegen der effizienten Kriminalitätsbekämpfung und der Gefahrenabwehr gerade im Bereich der Terrorismusbekämpfung fraglos unterstützungswürdig sind, scheint die Notwendigkeit einer Verlängerung der Aufbewahrungsdauer mindestens derzeit nicht ausgewiesen zu sein. Es leuchtet zwar ein, dass eine Verdoppelung derselben für die Strafverfolgungsbehörden eine Vereinfachung ihrer Ermittlungstätigkeit bedeuten dürfte, weil auch weiter zurückliegende Daten verwendet werden können. Dieser unbestreitbare Vorteil ist indessen den berechtigten Bedenken gegen die Verlängerung gegenüber zu stellen. Angesichts der Tatsache, dass auf europäischer Ebene dem Datenschutz und auch dem Recht auf Vergessen zunehmende Bedeutung zuerkannt werden[36] und in Deutschland über eine gar bloss siebentätige Aufbewahrungsfrist diskutiert wird,[37] erscheint die in der Schweiz verfolgte Einengung des Grundrechtsschutzes als problematisch.

C. Einsatz von sog. GovWare zur Überwachung

1. Begriff und Problematik

[Rz 19] Seit längerer Zeit schon existieren sog. Trojanische Pferde. Unter einem Trojanischen Pferd wird ein Computerprogramm verstanden, welches neben seiner eigentlichen Funktion auch weitere, unbekannte und vom Benutzer möglicherweise unerwünschte Funktionen aufweist. Insbesondere kann ein solches Programm Daten von der Festplatte des betroffenen Computers an einen Dritten senden oder Passwörter speichern und weiterleiten.[38] Die Möglichkeiten, ein solches Programm auf den Computer des Betroffenen einzuschleusen, sind mannigfaltig. Wurden solche Programme früher über Disketten verbreitet, steht heute der unbeabsichtigte Download vom Internet im Zentrum. Trojanische Pferde sind an sich kein neues Phänomen, erst in den letzten Monaten hat die Öffentlichkeit indessen erfahren, dass diese Software auch seitens staatlicher Behörden gezielt zur Überwachung von Verdächtigen eingesetzt worden ist.[39] Solche Fälle lassen sich unter dem Begriff GovWare zusammenfassen.

[Rz 20] GovWare ist vornehmlich entwickelt worden, um die Internetkommunikation von Verdächtigen zu überwachen. Im Vordergrund stand dabei das Programm Skype;[40] es sollte den Ermittlungsbehörden in erster Linie ermöglicht werden, über dieses Programm geführte Gespräche abzuhören. Damit beabsichtigt war, eine Lücke in der elektronischen Überwachung zu schliessen. Die bisherigen Möglichkeiten der Telefonüberwachung erlaubten es nämlich, von einem traditionellen Telefonanschluss geführte Kommunikation zu überwachen, über das Internet geführte Gespräche waren indessen davon ausgenommen. Die Funktionalität entsprechender Software ist indessen nicht zwingend auf die blosse Überwachung von ankommenden und abgehenden Gesprächen beschränkt; vielmehr ist es technisch auch möglich, die betroffenen Computer an sich auszuspionieren, d.h. in sich darauf befindliche Daten Einsicht zu nehmen.

[Rz 21] Im Rahmen der nachfolgend zu besprechenden Entzifferung des GovWare Programms durch den *Chaos Computer Club*[41] wurde sodann bekannt, dass neben der

[32] Art. 23 VE-revBÜPF.

[33] Art. 31 Abs. 1 lit. b VE-revBÜPF.

[34] Erläuternder Bericht zur Änderung des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) Ziff. 1.4.5 sowie 2.5; Art. 23.

[35] Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens über den Bericht und den Vorentwurf zur Änderung des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post Ziff. 5.4.

[36] Vgl. die Pressemitteilung der Europäischen Kommission vom 25. Januar 2012, abrufbar unter ‹http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&language=DE&guiLanguage=en›, besucht am 3. Februar 2012.

[37] Vgl. oben, Rz 12.

[38] Rolf H. Weber, E-Commerce und Recht, 2. Aufl., Zürich 2010, S. 539.

[39] Vgl. etwa «Der deutsche Staatstrojaner wurde geknackt», in Frankfurter Allgemeine Zeitung vom 8. Oktober 2011 (abrufbar unter ‹http://www.faz.net/aktuell/chaos-computer-club-der-deutsche-staatstrojaner-wurde-geknackt-11486538.html›, besucht am 27. Januar 2012); Zum Ganzen vgl. auch Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, in: Jusletter 5. Dezember 2011.

[40] Skype ist ein Computerprogramm, welches es dem Benutzer u.a. erlaubt, mit anderen Personen, welche ebenfalls im Besitze des Programmes sind, kostenlos zu telefonieren.

[41] Der Chaos Computer Club ist ein privatrechtlicher Verein, in welchem sich Hacker im deutschsprachigen Raum zusammengeschlossen haben.

Möglichkeit, den Kommunikationsverkehr abzuhören, auch andere Funktionen im betroffenen Programm enthalten waren oder aber mit minimalem Zusatzaufwand hinzugefügt werden konnten. Diese Funktionen sollten es etwa ermöglichen, auf Teile des betroffenen Computers zuzugreifen, gespeicherte Daten einzusehen und zu verändern sowie gar die eingebaute Kamera eines Computers per Fernsteuerung zu aktivieren.

2. Verwendung in der Schweiz und in Deutschland

[Rz 22] In den letzten Monaten sind verschiedene Fälle bekannt geworden, in welchen GovWare gezielt eingesetzt wurde, um verdächtige Personen zu überwachen. In der Schweiz haben die Behörden Medienberichten zufolge ein entsprechendes Programm zur Überwachung einer Linksaktivistin eingesetzt.[42] Des Weiteren gibt es offenbar Anhaltspunkte, dass Trojanische Pferde auch in weiteren Fällen zum Einsatz kamen.[43]

[Rz 23] In Deutschland berichtete der *Chaos Computer Club* im Oktober 2011, es sei ihm ein GovWare Programm zugespielt worden, welches seitens Polizeibehörden verwendet werde. Der *Chaos Computer Club* entschlüsselte und veröffentlichte sodann den Binärcode des fraglichen Programms.[44] Im Rahmen dieser Entzifferung stellte sich heraus, dass die bereitgestellten Funktionen der Software über das blosse Abhören von Kommunikation hinausgehen. Die Software wurde von den verschiedenen involvierten Behörden, namentlich den Verfassungsschutzbehörden, seit 2009 etwa 100-mal verwendet.[45] Ob die Veröffentlichung des Binärcodes für den *Chaos Computer Club* oder dessen Exponenten strafrechtliche Konsequenzen haben wird, ist – soweit ersichtlich – momentan noch unklar.[46]

3. Rechtliche Beurteilung

3.1. Derzeitige Rechtslage

[Rz 24] Unter dem Geltungsbereich der aktuellen eidgenössischen StPO ist es offenbar bisher zu keinem Einsatz von GovWare gekommen, die Anwendungsfälle in der Schweiz erfolgten noch unter Geltung der kantonalen Prozessordnungen.[47] Die eidgenössische StPO enthält keine gesetzliche Grundlage, welche den Einsatz von GovWare ausdrücklich erlauben würde.

[Rz 25] Mit Bezug auf den Einsatz von GovWare ist demnach zu differenzieren. Auf der einen Seite kann dieser bloss zur Überwachung von über den Computer geführten Gesprächen erfolgen, indem etwa das Programm Skype so manipuliert wird, dass eine Überwachung analog der Überwachung eines traditionellen Telefonanschlusses über eine Land- oder Mobilfunkverbindung möglich ist; diesfalls kommt es zur Aufzeichnung ohnehin stattfindender Vorgänge. Ein solcher Anwendungsfall lässt sich unter Art. 269 StPO subsumieren, indem von der statuierten Befugnis zur Überwachung von Post- und Fernmeldeverkehr Gebrauch gemacht wird.[48]

[Rz 26] Die übrigen möglichen Verwendungszwecke von GovWare, insbesondere also die Spionage über sich auf dem betroffenen Computer befindliche Dateien, sind indessen nicht von Art. 269 StPO erfasst, weil diese Norm bloss die eigentliche Überwachung des Fernmeldeverkehrs ermöglicht.[49] Als gesetzliche Grundlage für den Einsatz von GovWare in diesem Sinne könnte am ehesten Art. 280 StPO herangezogen werden, welcher die Überwachung mit technischen Überwachungsgeräten erlaubt; die Anwendung dieser Bestimmung für die Rechtfertigung des Einsatzes von GovWare bedeutet aber fraglos, sie zu strapazieren, weil sie auf einen solchen Anwendungsfall an sich nicht ausgelegt ist.[50] Ein ohne Rechtfertigung ausgeführter Eingriff in einen fremden Computer dürfte somit unter der geltenden Rechtslage und sofern die übrigen Tatbestandsvoraussetzungen erfüllt sind, den Tatbestand des unbefugten Eindringens in ein Datenverarbeitungssystem[51] erfüllen. Konsequenz daraus ist neben der strafrechtlichen Verantwortlichkeit der betroffenen Personen insbesondere, dass die entsprechend erlangten Erkenntnisse nach Art. 141 StPO als unverwertbar anzusehen und dementsprechend in einem Strafverfahren nicht verwendbar sind. Demgemäss erscheint es, wenn der Einsatz von GovWare möglich gemacht werden soll, als unausweichlich, eine ausdrückliche gesetzliche Grundlage dafür zu schaffen.

[Rz 27] In Deutschland hatte das Bundesverfassungsgericht

---

[42] Vgl. ««Staatstrojaner» im Fall Stauffacher eingesetzt», Neue Zürcher Zeitung vom 15. Oktober 2011 (abrufbar unter ‹http://www.nzz.ch/nachrichten/politik/schweiz/trojaner_im_fall_stauffacher_eingesetzt_1.12994241.html›, besucht am 3. Februar 2012).

[43] Vgl. N 43, a.a.O.

[44] Vgl. ‹http://ccc.de/de/updates/2011/staatstrojaner›, besucht am 3. Februar 2012.

[45] Vgl. ‹http://www.spiegel.de/netzwelt/netzpolitik/0,1518,791941,00.html›, besucht am 3. Februar 2012.

[46] Vgl.etwa‹http://www.mz-web.de/servlet/ContentServer?pagename=ksta/page&atype=ksArtikel&aid=1319025291186&calledPageId=987490165154›, besucht am 3. Februar 2012.

[47] Vgl. «Unklare Rechtsgrundlage», Neue Zürcher Zeitung vom 14. Oktober 2011.

[48] Beat Rhyner / Dieter Stüssi, in: Albertini, Fehr, Voser, (Hrsg.): Polizeiliche Ermittlung, Zürich 2008, S. 469.

[49] Gl. M. Hansjakob Thomas, N 14 zu Art. 269, in: Donatsch, Thomas, Lieber (Hrsg.); Ders. Einsatz von GovWare – zulässig oder nicht?, in: Jusletter 5. Dezember 2011 Rz 18; Kommentar zur Schweizerischen Strafprozessordnung (StPO), Zürich 2010.

[50] Hansjakob Thomas, N 2 zu Art. 280, in Donatsch, Thomas, Lieber (Hrsg.); Niklaus Schmid. Schweizerische Strafprozessordnung (StPO) : Praxiskommentar, Zürich 2009 N 8 zu Art. 280; Mark Pieth, Schweizerisches Strafprozessrecht, Basel 2009, S. 132.

[51] Art. 143bis StGB.

im Jahre 2008 zu beurteilen, ob Vorschriften des Nordrhein-Westfälischen Verfassungsschutzgesetzes, welche den Zugriff auf informationstechnische Systeme erlaubten, mit dem Grundgesetz, der deutschen Verfassung, vereinbar seien. Während die dabei in Frage stehende Regelung im konkreten Fall als verfassungswidrig und demnach nichtig erklärt wurde, hielt das Bundesverfassungsgericht allgemein fest, dass die Verwendung von GovWare nur, aber immerhin dann zulässig sei, wenn *tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen*.[52] Des Weiteren bedürfe der Einsatz von GovWare einer richterlichen Bewilligung.[53] Während im Rahmen der konkret in Frage stehenden Norm diese Einschränkungen nicht vorgesehen gewesen waren, müsste eine Regelung, welche den statuierten Anforderungen genügt, in diesem Sinne als verfassungsmässig und damit zulässig erachtet werden.

3.2. Handlungsbedarf in der Schweiz?

[Rz 28] Wie bereits dargelegt, sieht der VE-BÜPF die Schaffung eines neuen Art. 270bis StPO vor, welcher das Einführen von Informatikprogrammen in ein Datensystem zum Abfangen und Lesen von Daten ausdrücklich regeln soll. Eine solche gesetzliche Regelung ist im Gegensatz zum derzeitigen Rechtszustand, in welchem es als fraglich erscheint, ob der Einsatz rechtmässig ist, deshalb begrüssenswert, weil eine Klarstellung erfolgt. Ob indessen den Strafverfolgungsbehörden die entsprechenden Möglichkeiten eingeräumt werden sollen, ist eine kontrovers beurteilte Frage.

[Rz 29] Im Rahmen der Vernehmlassungsergebnisse zum VE-BÜPF wurde denn auch deutlich, dass diesbezüglich die Meinungen stark auseinander gehen. Während einige Vernehmlassungsteilnehmer sich grundsätzlich für die Möglichkeit des Einsatzes von GovWare aussprachen, erachteten andere diesen als einen zu schweren Eingriff in die Privatsphäre der Betroffenen, welcher entweder gar nicht oder aber nur unter strengeren Bedingungen zulässig sein sollte.[54] So wird insbesondere – in Anlehnung an das diesbezügliche Urteil des deutschen Bundesverfassungsgerichts[55] – die Beschränkung des Deliktskataloges derjenigen Straftaten, angesichts welcher ein GovWare-Programm verwendet werden darf, verlangt.[56] Weitere Forderungen beinhalten angesichts des Schädigungspotentials entsprechender Programme eine ausdrückliche Haftung des Bundes für entstandene Schäden sowie den Verzicht auf Programme, welche die Funktionalität anderer Programme beeinträchtigen. Die Einführung einer neuen Norm hat u.E. enge Voraussetzungen für den Einsatz von GovWare zu formulieren.

[Rz 30] Eine ausdrückliche Regelung des Einsatzes von GovWare war des Weiteren auch für die präventive Bekämpfung von Verbrechen vorgesehen. Der VE-revBWIS[57] sah in Art. 18n vor, dass in besonderen Situationen eine Durchsuchung eines fremden Datenverarbeitungssystems erfolgen könne. Bemerkenswert an der Formulierung des VE-revBWIS war vor allem der Umstand, dass explizit die Durchsuchung des betroffenen Datenverarbeitungssystems vorgesehen war, also eine bewusst über die blosse Überwachung von Gesprächen hinausgehende Möglichkeit eines Eingriffs in private Datensysteme statuiert wurde.[58] Im Laufe des politischen Prozesses hat das Parlament jedoch den beantragten Änderungen der sog. Besonderen Informationsbeschaffung, welche u.a. den oben dargelegten Einsatz ermöglicht hätte, eine Absage erteilt.[59] Die kürzlich verabschiedete Referendumsvorlage[60] sieht deshalb in sachgerechter Weise keine entsprechende Möglichkeit mehr vor.[61]

D. Geolokalisierungsdienste

1. Begriff und Problematik

[Rz 31] Geolokalisierungsdienste ermöglichen es den Interessierten, die Position eines Betroffenen aufgrund des Standortes seines Mobiltelefons oder des verwendeten Computers zu bestimmen. Involviert sind verschiedenste Interessen: (i) Die Standortbestimmung kann im Dienste des öffentlichen Interesses erfolgen, etwa zur Kriminalitätsbekämpfung oder zur Suche nach vermissten Personen.[62] (ii) Unternehmen sind zu Marketingzwecken an Geolokalisationsdaten interessiert. (iii) Location based services im Rahmen sozialer Netzwerke bieten den Nutzern die Möglichkeit, sich an einem bestimmten Ort unter Verwendung der Standortbestimmung des Mobiltelefons anzumelden.

---

[52] Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 in den Rechtssachen 1 BvR 370/07 und 1 BvR 595/07 , abrufbar unter ‹http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html›, besucht am 31. Januar 2012.

[53] Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 (N 53), Leitsätze 2 und 3.

[54] Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens über den Bericht und den Vorentwurf zur Änderung des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post, Ziff. 11.1.2.

[55] Vgl. Fn. 53.

[56] Vgl. Fn. 55

[57] Auch BWIS II genannt.

[58] Vgl. den Wortlaut von Art. 18n VE-revBWIS sowie den Erläuternden Bericht zum Vorentwurf fedpol vom 31. Januar 2006 zum Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS), Ziff. 2.34.

[59] Nicheintretensentscheid Nationalrat: AB NR 2008, 1892 sowie AB NR 2009, 676; Der Ständerat hat Eintreten auf die Vorlage beschlossen: AB SR 2009, 21 (vgl. auch Art. 87 Abs. 2 ParlG).

[60] Ablauf der Referendumsfrist am 13. April 2012.

[61] Zusatzbotschaft zur Änderung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit, BBl 2010 7851. Vgl. aber auch den Plan einer neuerlichen Revision wie dargelegt in: «neue Leitplanken für den Staatsschutz», Neue Zürcher Zeitung Nr. 34 vom 10. Februar 2012, S. 9; «Jetzt kommt der grosse Lauschangriff», Tages-Anzeiger Nr 33 vom 9. Februar 2012, S. 1 und 5.

[62] Art. 3 BÜPF.

[Rz 32] Erfolgt die Anmeldung (sog. Check-in) hinsichtlich eines Geschäfts oder Restaurants, wird sie teilweise mit Vergünstigungen oder anderen Vorteilen für den Betroffenen belohnt. Kommerzielle Akteure erhoffen sich durch die Anmeldung einen besonderen Werbeeffekt im Rahmen der Mund-zu-Mund Propaganda. Gefahren bzw. Vorbehalte gegenüber Geolokalisierungsdiensten umfassen neben den allgemeinen datenschutzrechtlichen Fragestellungen insbesondere auch den Umstand, dass die Preisgabe des aktuellen Standortes sowie ggf. der Alltagsgewohnheiten für Kriminelle nützlich sein könnte, indem diese Zeiten, zu welchen sich der Betroffene an einem bestimmten Ort aufhält, etwa zur Planung eines Einbruches oder zum Zwecke des Stalkings genutzt werden könnten.[63]

[Rz 33] Technisch ist die Ortung des Betroffenen über verschiedene Kanäle möglich. Moderne Mobiltelefone – smartphones – verfügen oft über eingebaute GPS-Module, mit welchen der jeweilige Standort mit hohem Genauigkeitsgrad bestimmt werden kann. Unterstützend, sowie bei den übrigen Mobiltelefonen ausschliesslich, kann die Position auch über die verwendete Funkzelle des Mobiltelefons erfolgen. Dabei ist allerdings die Ortung weniger genau als bei GPS-Sendern. Mittels des sog. Triangulationsverfahrens lässt sich indessen ebenfalls eine verhältnismässig genaue Ortung vornehmen.[64] Bei ortsgebundenen Geräten ist sodann eine Ortung über die IP-Adresse denkbar. Weitere Möglichkeiten der Geolokalisierung, deren Behandlung indessen den Rahmen des vorliegenden Beitrages sprengen würde, stellen die Verwendung von RFID-Chips[65] sowie die Dokumentation von Aufenthaltsorten mittels bildtechnischen Mitteln, etwa Überwachungskameras, dar.

[Rz 34] Angesichts der zu erwartenden weiteren Verbreitung von Mobiltelefonen mit Ortungsfunktion kann davon ausgegangen werden, dass die Sammlung entsprechender Daten in näherer Zukunft zunehmen wird. Dadurch dürfte es schwieriger werden, sich der Möglichkeit der Ortung zu entziehen, indem verschiedene Dienstleistungsanbieter ihre Leistungen standardmässig mit einer Lokalisierungsfunktion versehen und teilweise gar nur noch erbringen, wenn der betroffene Nutzer sich geographisch orten lässt. Deshalb ist zu hinterfragen, inwiefern die Erhebung entsprechender Daten sich mit den rechtlichen Rahmenbestimmungen vereinbaren lässt und welche Schranken solchen Diensten gesetzt sind.

2. Rechtslage in der Schweiz

2.1 Derzeitige Rechtslage

[Rz 35] Das Angebot von Ortungsdiensten untersteht – sofern nicht eine Anordnung der Standortbestimmung durch staatliche Behörden in Frage steht[66] – den Vorschriften des FMG sowie des DSG. Das Bundesgesetz über die Geoinformation (Geoinformationsgesetz) hingegen findet auf Ortungsdienste im hier verstandenen Sinne keine Anwendung.[67]

[Rz 36] Art. 45b FMG bestimmt, dass Fernmeldedienstanbieter die Standortdaten nur für eigene Dienste und die Abrechnung verwenden dürfen. Zu den Standortdaten zählen diejenigen Daten, welche über den aktuellen oder den zu einem bestimmten vergangenen Zeitpunkt bestehenden Standort des betroffenen Gerätes Auskunft geben. Im Gegensatz zu den Randdaten sagen sie nichts über die tatsächliche Verwendung des betroffenen Geräts aus. Eine weitergehende Nutzung bzw. Bearbeitung ist, es sei denn, diese geschehe anonym, nur mit vorgängiger Einwilligung des Betroffenen möglich. Die Verwendung von Ortungsdiensten im vorliegend interessierenden Rahmen setzt stets ein aktives Tun des Betroffenen voraus. Die Benutzung der fraglichen Dienste[68] bedarf daher stets der Zustimmung des betroffenen Nutzers. Weil die Verweigerung der Zustimmung in der Regel den Zugriff auf die angebotenen Dienstleistungen verunmöglicht oder gewisse Funktionalitäten des Dienstes ausschaltet, kann im Willen der Nutzung der Dienste eine Zustimmung des Betroffenen gesehen werden.

[Rz 37] Die durch die Geolokalisierung gewonnenen und verarbeiteten Angaben beziehen sich, wenn sie nicht anonymisiert sind, auf eine bestimmte Person, nämlich den in Frage stehenden Nutzer. Demnach stellen sie Personendaten im Sinne von Art. 3 lit. a DSG dar und fallen in den DSG-Schutzbereich. Bei nicht bloss vereinzelter Nutzung der Geolokalisierungsdienste kann sogar ein Persönlichkeitsprofil im Sinne von Art. 3 lit. d DSG entstehen, indem die Zusammenstellung der Daten die Beurteilung wesentlicher Aspekte der Persönlichkeit des Betroffenen erlaubt.

[Rz 38] Die Bearbeitung entsprechender Lokalisierungsdaten untersteht dementsprechend den allgemeinen Bestimmungen des DSG. Aus diesem Grunde darf die Verwendung der durch die Geolokalisierung generierten Daten nur in rechtmässiger Weise und nur nach Treu und Glauben erfolgen.[69] Zweifelhaft sein kann insbesondere, ob die Zweckbindung der Datenbearbeitung[70] der Verwendung der generierten Daten durch den Dienstleistungsanbieter Grenzen zu setzen vermag. Das Interesse des Nutzers an der Freigabe

[63] Geolokalisierung per Handy, in datum 02/2010.

[64] Beim Triangulationsverfahren wird die Verbindung zu zwei oder mehr Mobilfunkantennen zur Bestimmung des genauen Standortes gemessen.

[65] RFID steht für *Radio-Frequency Identification*. Darunter zu verstehen ist die Identifikation von Gegenständen und Personen mittels elektromagnetischer Wellen.

[66] Für diesen Fall sei auf die obigen Ausführungen verwiesen.

[67] Art. 2 und 3 GeoIG.

[68] Etwa Facebook Places, Foursquare, Qype oder Twitter.

[69] Art. 4 Abs. 1 und 2 DSG.

[70] Art. 4 Abs. 3 und 4 DSG.

der fraglichen Angaben liegt in aller Regel in der Mitteilung an Freunde, ggf. in der Erlangung spezieller Vergünstigungen durch die Nutzung. Die Möglichkeit, dass sich über den Nutzer der Dienstleistung bei regelmässiger Verwendung ein eigentliches Persönlichkeitsprofil erstellen lässt, dürfte von den meisten Nutzern nicht gewünscht sein. Auch lässt sich davon ausgehen, dass die meisten Nutzer entsprechender Dienstleistungen nicht daran denken, dass die über sie generierten Daten auch nach der Bereitstellung des konkret in Frage stehenden Inhalts für weitere Zwecke gespeichert werden. Der Grundsatz von Treu und Glauben der Datenverarbeitung setzt den Dienstleistungsanbietern demnach entsprechende Grenzen der Verwendung. In zeitlicher Hinsicht ist der Dienstleistungsanbieter ebenfalls an die allgemeinen Grundsätze der Datenbearbeitung gebunden, welche ihm die Aufbewahrung der generierten Daten länger als für die verfolgten, rechtmässigen Zwecke nötig verbietet.

2.2 Handlungsbedarf in der Schweiz?

[Rz 39] Das derzeitige Datenschutzrecht beschäftigt sich nicht ausdrücklich mit der Frage der Verwendung von Geolokalisierungsdaten, ausgenommen die Norm von Art. 45b FMG, welche den wichtigen Grundsatz der vorgängigen Einwilligung durch den Betroffenen statuiert. Was indessen mit den einmal erhobenen Lokalisierungsdaten passiert, richtet sich – im Rahmen der allgemeinen Datenschutzbestimmungen – nach der entsprechenden Nutzungsvereinbarung. Es obliegt damit in erster Linie den Parteien, eine vertragliche Beschränkung der Datenverarbeitung vorzusehen.

[Rz 40] Weil die Nutzer sich der abgeschlossenen Vereinbarung indessen häufig kaum bewusst sind – ist doch die Zustimmung zu den Bestimmungen durch ein einfaches Anklicken eines Kästchens erledigt – erscheint es als wünschenswert, dass der Datenbearbeitung von Lokalisierungsdaten gewisse Grenzen gesetzt werden. Die allgemeinen Datenschutzprinzipien greifen im Hinblick auf die Geolokalisierung zu kurz. Dies liegt vor allem darin begründet, dass die einzelnen Daten für sich und damit im Zeitpunkt der Erhebung keine wesentlichen Informationen enthalten, sich deren Sinngehalt und insbesondere auch die Möglichkeit der Erstellung eines Persönlichkeitsprofils erst durch das Zusammenspiel verschiedener Anwendungen ergibt.

E. Ausblick

[Rz 41] Die Gefahrenabwehr und die Kriminalitätsbekämpfung brauchen fraglos die Möglichkeit, bei entsprechendem Bedarf auf gewisse Daten des Betroffenen zugreifen zu können. Die zeitlichen Grenzen einer voraussetzungslosen Vorratsdatenspeicherung in der Schweiz erscheinen im europäischen Durchschnitt derzeit als angemessen. Die sechsmonatige Aufbewahrungsdauer dürfte wohl in den allermeisten Fällen den beabsichtigten Zweck, nämlich die erst nach Verübung eines Delikts vorzunehmende Identifizierung, zufriedenstellend erlauben. Dass das Bedürfnis nach einer Erhöhung dieser Frist ausgewiesen ist, erscheint zum jetzigen Zeitpunkt kaum als ausgewiesen. Deshalb drängt sich unter Berücksichtigung des dadurch erfolgenden schweren Eingriffes in das informationelle Selbstbestimmungsrecht der Betroffenen eine Verlängerung der Aufbewahrungsfrist nicht auf.

[Rz 42] Die ausdrückliche Regelung der Zulassung sowie der Anwendungsfelder von sog. GovWare ist zu begrüssen. Momentan besteht in diesem Zusammenhang eine unbefriedigende gesetzliche Regelung, weil unklar ist, ob und wie weit eine solche Massnahme ergriffen werden darf. Gerade in Anbetracht des sich aus einer solchen Verwendung ergebenden Schädigungspotentials, aber auch der absehbaren damit einhergehenden Steigerung der Verbrechensaufklärung ist es unumgänglich, dass sich der Gesetzgeber zum Einsatz und den damit verbundenen Voraussetzungen äussert. Ob der entsprechende Zugriff schliesslich erlaubt wird, ist eine politische Frage, bei welcher die Vor- und Nachteile solcher Massnahmen gegeneinander abzuwägen sind. Auf jeden Fall ist indessen zu fordern, dass die möglichen Anwendungsfelder klar umrissen sind sowie ein angemessener Schutz gegen den möglichen Missbrauch und mögliche Schädigungen durch die Verwendung von GovWare statuiert wird.

[Rz 43] Die Verwendung von Geolokalisierungsdiensten stellt die Datenschutzgesetzgebung vor noch ungelöste Probleme. Auf der einen Seite besteht das insoweit legitime Bedürfnis der Nutzer von entsprechenden Diensten, auf ihren Standort zugeschnittene Informationen zu erhalten, sowie ein Interesse der Anbieter solcher Dienste, derartige Angebote unterbreiten zu können. Problematisch gestaltet sich auf der anderen Seite indessen die längerfristige Sammlung der entsprechenden Daten. Die Bestimmung der örtlichen Aufenthaltsorte einer Person während ihres Tagesablaufes ist in der Regel geeignet, hinsichtlich des Betroffenen ein relativ klares Bild über die Person an sich, ihre Vorlieben und Handlungsweisen zu vermitteln. Die Datenschutzgesetzgebung hat die Entwicklungen in diesem Bereich aufmerksam im Auge zu behalten, um bei entsprechendem Bedürfnis Abhilfe schaffen zu können, etwa durch die Festlegung von Grenzen der Aufbewahrung entsprechender Daten oder einer vereinfachten Löschungsmöglichkeit für die Betroffenen.

Prof. Dr. Rolf H. Weber, Ordentlicher Professor an der Universität Zürich, Gastprofessor an der University of Hong Kong, Rechtsanwalt in Zürich

Christoph A. Wolf, lic.iur., Wissenschaftlicher Assistent Universität Zürich

Ulrike I. Heinrich, Rechtsanwältin (Berlin), Wissenschaftliche Assistentin Universität Zürich

---